**UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**

| | | |
|---|---|---|
| PARAMOUNT PICTURES CORPORATION, a Delaware corporation, Plaintiff, | ) | |
| v. | ) | Case No.: 05-11588-RWZ |
| JOHN DOE, Defendant. | ) | |

**DECLARATION OF THOMAS CARPENTER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE**

I, Thomas Carpenter, declare:

1. I am Director, Data Services for MediaSentry business unit of SafeNet Inc. ("MediaSentry"), where I have been employed since January 2005. MediaSentry is a leading provider of online anti-piracy services for the motion picture, music, game and business software, and print publishing sectors. Before my employment with MediaSentry, I held various senior level positions at companies that developed Internet based technologies and have approximately ten years of experience related to the protocols, technical architecture and operation of the Internet.

2. I submit this declaration in support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

3. MediaSentry has developed a technology platform that provides an effective means to detect unauthorized distribution of digital music, software, games, content, and movies over online media distribution systems, or "peer-to-peer" ("P2P") networks. At MediaSentry, I am the head of the department that carries out evidence collection using a platform known as

"MediaTarget." I work closely with our development team to create credible techniques to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners.

4. MediaSentry was hired on behalf of Plaintiff to monitor and identify copyright infringement of specified motion pictures on P2P networks. Under direct supervision of Plaintiff's counsel, MediaSentry engaged in a specific process utilizing specially designed software and other technology to identify direct infringers of Plaintiff's copyrights on P2P networks.

5. Plaintiff provided MediaSentry with a list of copyrighted motion pictures they believe may be offered for distribution on P2P networks.

6. MediaSentry connects to various P2P networks and searches for users who are offering one or more of Plaintiff's specified motion pictures. MediaSentry uses the same core technical processes that are used by P2P users to identify users who are offering Plaintiff's motion pictures over the Internet. Any user of a P2P network can obtain any of the information that is obtained by MediaSentry from the P2P network.

7. Once MediaSentry's searching software program identifies a P2P network user that is offering for download one of the specified motion pictures, it obtains the Internet Protocol ("IP") address of that user, and when available, it obtains the user's screen name and examines the user's publicly available directory on his computer for other files that lexically match the motion pictures on Plaintiff's list. Viewing a user's shared directory is a functionality that is built into many, but not all, of the P2P protocols for the relevant P2P service. MediaSentry then downloads at least one motion picture that the user is offering.

8. In addition to the file of the motion picture itself, MediaSentry downloads other publicly available information from the network user that is designed to help Plaintiff identify the user. Among other things, MediaSentry downloads or records for each file downloaded from each user: (a) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to the digital file and helps identify the

content of the file; (b) the time and date at which the file was downloaded from the user; and (c) the IP address assigned to each user at the time of infringement. MediaSentry then creates evidence logs for each user that store all this information in a central database.

9. An IP address is a unique numerical identifier that is automatically assigned to a user by its Internet Service Provider ("ISP") each time a user logs on to the network. Each time a subscriber logs on, he or she may be assigned a different IP address. ISPs are assigned certain blocks or ranges of IP addresses. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such "user logs" for a limited amount of time. These user logs provide the most accurate means to connect an infringer's identity to its infringing activity.

10. Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable via the use of a packet "sniffer." A computer operator's "sniffer" is a type of software program that can be used to identify IP addresses connected to the operator's computer by virtually "sniffing" packets of information shared over a P2P network. Such applications are widely available to the public and do not require a great degree of sophistication to operate. Furthermore, any computer running on Microsoft Windows is equipped with a utility to display IP addresses currently connected to it. MediaSentry uses such a "sniffing" application to ascertain users' IP addresses.

11. An infringer's IP address is significant because it is a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable MediaSentry to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables MediaSentry to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

12. Here, the IP address identified by MediaSentry via the use of a packet sniffer enabled us to determine which ISP was used by each infringer to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship -- customer, contractual, or otherwise -- with the end-user, they are unable to identify the Doe Defendant through reference to their user logs. The intermediary ISPs' own user logs, however, should permit identification of the Doe Defendant.

13. Using a packet sniffer, MediaSentry determined that the Doe Defendant here was using Massachusetts Institute of Technology ("MIT") to gain access to the Internet and distribute and make available for distribution and copying the copyrighted motion pictures identified. MediaSentry downloaded the motion picture file and other identifying information described above and created an evidence log for the Doe Defendant. Once MediaSentry identified the ISP used by the Doe Defendant to gain access to the Internet from the IP address, Plaintiff's counsel, using the MediaSentry application, sent an e-mail to the relevant contact at MIT informing him or her of the Doe Defendant's IP address and the date and time of the infringing activity. That e-mail message requested that MIT retain the records necessary to identify its subscriber who was assigned that IP address at that date and time. Once provided with the IP address, plus the date and time of the infringing activity, the Doe Defendant's ISP quickly and easily can use its subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time..

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 29 July, 2005, at Morristown, NJ.

Thomas Carpenter